

(12) 特許協力条約に基づいて公開された国際出願

(19) 世界知的所有権機関
国際事務局

(43) 国際公開日
2014年2月27日(27.02.2014)



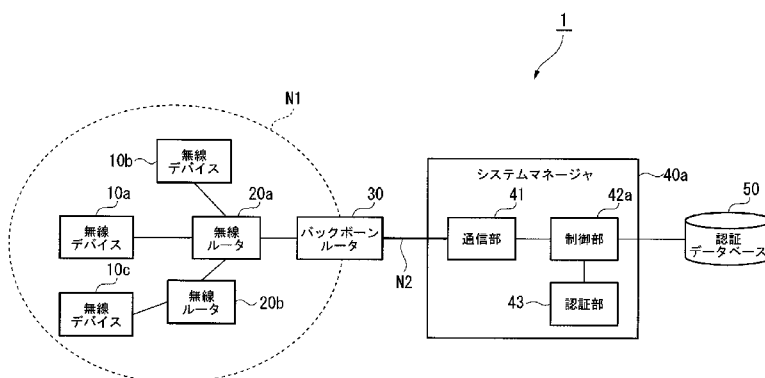
(10) 国際公開番号
WO 2014/030669 A1

- (51) 国際特許分類:
H04L 9/32 (2006.01) *H04W 12/06* (2009.01)
- (21) 国際出願番号: PCT/JP2013/072285
- (22) 国際出願日: 2013年8月21日(21.08.2013)
- (25) 国際出願の言語: 日本語
- (26) 国際公開の言語: 日本語
- (30) 優先権データ:
特願 2012-182297 2012年8月21日(21.08.2012) JP
- (71) 出願人: 横河電機株式会社(YOKOGAWA ELECTRIC CORPORATION) [JP/JP]; 〒1808750 東京都武蔵野市中町2丁目9番32号 Tokyo (JP).
- (72) 発明者: 宮澤 和紀(MIYAZAWA Kazunori); 〒1808750 東京都武蔵野市中町2丁目9番32号 横河電機株式会社内 Tokyo (JP). 秋定 征世(AKISADA Yukiyo); 〒1808750 東京都武蔵野市中町2丁目9番32号 横河電機株式会社内 Tokyo (JP). 櫻井 康樹(SAKURAI Yasuki); 〒1808750 東京都武蔵野市中町2丁目9番32号 横河電機株式会社内 Tokyo (JP).
- (74) 代理人: 志賀 正武, 外(SHIGA Masatake et al.); 〒1006620 東京都千代田区丸の内一丁目9番2号 Tokyo (JP).
- (81) 指定国 (表示のない限り、全ての種類の国内保護が可能): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, KE, KG, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.
- (84) 指定国 (表示のない限り、全ての種類の広域保護が可能): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, SZ, TZ, UG, ZM, ZW), ユーラシア (AM, AZ, BY, KG, KZ, RU, TJ, TM), ヨーロッパ (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).
- 添付公開書類:
— 国際調査報告 (条約第21条(3))

(54) Title: AUTHENTICATION SYSTEM, MANAGEMENT DEVICE, AND AUTHENTICATION METHOD

(54) 発明の名称: 認証システム、管理装置及び認証方法

[図1]



10a, 10b, 10c Wireless device
20a, 20b Wireless router
30 Backbone router
40a System manager
41 Communication unit
42a Control unit
43 Authentication unit
50 Authentication database

(57) Abstract: This management device is equipped with: a communication unit for receiving connection requests from communication devices connected to a network; a control unit that reads from a database a first certificate for authenticating a communication device that has made a communication request when the request is received by the communication unit; and an authentication unit for authenticating the communication device that has transmitted the connection request by using the first certificate read by the control unit.

(57) 要約: 管理装置は、ネットワークに接続される通信デバイスからの接続要求を受信する通信部と、通信部が接続要求を受信した場合に、接続要求を行った通信デバイスを認証するための第1証明書と、データベースから読み出す制御部と、制御部が読み出した第1証明書を用いて、接続要求を送信した通信デバイスの認証を行う認証部と、を備える。

明 細 書

発明の名称： 認証システム、管理装置及び認証方法

技術分野

[0001] 本発明は、ネットワークに接続される通信デバイスの認証を行う認証システム、管理装置及び認証方法に関する。

本願は、2012年8月21日に、日本に出願された特願2012-182297号に基づき優先権を主張し、その内容をここに援用する。

背景技術

[0002] 従来から、プラントや工場等においては、高度な自動操業を実現すべく、分散制御システム（DCS：Distributed Control System）が構築されている。この分散制御システムでは、フィールド機器と呼ばれる現場機器（測定器、操作器）と、これらの制御を行う制御装置とが通信手段を介して接続される。このような分散制御システムの基礎をなす通信システムは、有線によって通信を行うものが殆どであった。しかし、近年においてはISA100.11aやWirelessHART（登録商標）等の産業用無線通信規格に準拠した無線通信を行うものも実現されている。

[0003] 上記の通信システムには、セキュリティを確保するために、PKI（Public Key Infrastructure：公開鍵基盤）を用いて有線又は無線のネットワークに接続される通信デバイスを認証する認証システムが設けられる。とりわけ、無線ネットワークを介して通信を行う通信システムでは、通信デバイス（無線デバイス）が電波の到達エリア内に配置されていれば無線ネットワークに接続し得る。そのため、無線ネットワークを介して通信を行う通信システムでは、セキュリティを確保する観点から上記の認証システムは必須になる。

[0004] ここで、上記の認証システムは、信頼できる認証局（CA：Certification Authority）が発行した証明書を管理するとともに、この証明書を用いて通信デバイスの認証を行う管理装置を備える。具体的に、この管理装置は、通

信デバイスから提示される証明書の正当性を、自らが管理している証明書を用いて検証した上で、通信デバイスとの間でチャレンジ・レスポンス方式によりデータ（メッセージ）の送受信を行う。これにより、管理装置は、通信デバイスの認証を行う。

- [0005] 尚、通信デバイスが管理装置に対して証明書を提示する方法として、第1方式（ピギーバック（PiggyBack）方式）と、第2方式（匿名接続方式）とが挙げられる。第1方式では、ネットワークへの接続要求（ジョイン要求）とともに証明書を提示する。第2方式では、ネットワークに対して匿名接続を行っている最中に証明書を提示する。以下の特許文献1には、プラントや工場等に設けられる認証システムで用いられるものではないが、従来のPKIを用いたチャレンジ・レスポンス認証方法が開示されている。

先行技術文献

特許文献

- [0006] 特許文献1：特開2008-167107号公報

発明の概要

発明が解決しようとする課題

- [0007] 上述した認証局から通信デバイス（認証システムの管理装置によって認証を受ける通信デバイス）に付与される証明書は、一般的にセキュリティを高めるために有効期限が設定される。このような有効期限が設定された証明書が用いられる場合には、その有効期限が経過する前に、ネットワークを介した安全な通信（セキュアな通信）によって証明書を更新する必要がある。
- [0008] しかしながら、プラントや工場等で用いられるフィールド機器等の通信デバイスは、出荷された後で直ちに用いられるもの以外に、予備として長期間保管されるものもある。このような通信デバイスは、保管中に証明書の有効期限が経過してしまうと、ネットワークに接続することができなくなる。上述の通り、証明書の更新は、ネットワークを介した通信により行われる。そのため、証明書の有効期限の経過によってネットワークに接続できなくなる

と、証明書の更新も行うことができなくなる。このため、従来は、ネットワークに接続される可能性のある全ての通信デバイスについて証明書の期限管理をしなければならず、極めて煩雑な手間を要する。

[0009] また、上述した無線通信規格 I S A 1 0 0 . 1 1 a 等に準拠した無線ネットワークは、電池を電源として間欠動作を行う無線デバイス（無線フィールド機器）や無線ルータ等によって形成される。そのため、省電力で低速（通信帯域が狭い）であるという特質を有する。このような特質から、上記の無線ネットワークを介して送受信されるパケットの大きさは、百バイト程度（例えば、128バイト）に制限される。無線デバイスで測定された圧力、流量、温度等のプロセス量を示すデータは、このパケットを単位として通信される。

[0010] しかしながら、無線デバイスの認証に用いられる証明書は、データ量が数キロバイト程度以上であり、上記のプロセス量を示すデータに比べてデータ量が多い。このため、無線デバイスから管理装置に対して証明書を送信するためには、多くのリソースが必要である。そのため、証明書を送信する無線デバイスと管理装置との間の通信経路上に配置された無線ルータ等の無線デバイスのリソースが多く消費される。これにより、電池の交換時期が早まったり、本来のプロセス量のデータ送信に支障が生じたりする可能性がある。

[0011] 本発明は、通信デバイスの認証に用いられる証明書の管理を簡素化することができるとともに、証明書の送受信に要するリソースを削減することができる認証システム、管理装置及び認証方法を提供する。

課題を解決するための手段

[0012] （１） 本発明の第１の態様は、第１ネットワークに接続される通信デバイスを認証するために用いられる第１証明書を格納するデータベースと、前記通信デバイスからの接続要求があった場合に、前記接続要求を行った前記通信デバイスを認証するための第１証明書を前記データベースから読み出し、第１証明書を用いて、前記接続要求を行った前記通信デバイスの認証を行う管理装置と、を備える認証システムである。

本発明の第１の態様によると、通信デバイスからの接続要求があった場合に、その接続要求を行った通信デバイスを認証するための第１証明書がデータベースから読み出され、読み出された第１証明書を用いて接続要求を行った通信デバイスの認証が管理装置によって行われる。

[0013] (２) 本発明の第１の態様において、前記データベースに格納される前記第１証明書は、前記第１証明書を検証するための第２証明書を用いて検証されても良い。

[0014] (３) 本発明の第１の態様において、前記第１ネットワークとは異なる第２ネットワークを介して前記管理装置に接続され、前記データベースに格納された情報を提供するサーバ装置を更に備え、前記管理装置は、前記サーバ装置から前記データベースに格納された前記第１証明書を取得されても良い。

[0015] (４) 本発明の第１の態様において、前記データベースに格納される前記第１証明書を発行する認証局サーバ装置を更に備えても良い。

[0016] (５) 本発明の第１の態様において、前記通信デバイスには、前記第１証明書が付与されており、前記管理装置は、前記接続要求を行った前記通信デバイスを認証するための前記第１証明書が前記データベースに格納されていない場合には、前記接続要求を行った前記通信デバイスに付与されている前記第１証明書を取得して、前記接続要求を行った前記通信デバイスの認証を行っても良い。

[0017] (６) 本発明の第１の態様において、前記第１ネットワークは、無線ネットワークであり、前記第２ネットワークは、前記第１ネットワークよりも通信帯域が広くても良い。

[0018] (７) 本発明の第１の態様において、前記データベースは、前記第１証明書と、前記通信デバイスを一意に特定する識別子とを対応付けて格納し、前記管理装置は、前記通信デバイスから、前記接続要求と、前記通信デバイスを一意に特定する識別子とを受信する通信部と、前記通信部が受信した前記識別子に対応付けられた前記第１証明書を、前記データベースから読み出す

制御部と、前記制御部が読み出した前記第 1 証明書を用いて前記接続要求を行った前記通信デバイスの認証を行う制御部と、を備えても良い。

[0019] (8) 本発明の第 1 の態様において、前記認証部は、前記第 1 証明書に含まれる第 1 公開鍵を用いて第 1 メッセージを暗号化し、前記通信部は、前記認証部が暗号化した前記第 1 メッセージを、前記通信デバイスに送信し、前記通信部は、第 2 公開鍵を用いて暗号化された第 2 メッセージを、前記通信デバイスから受信し、前記認証部は、前記第 2 メッセージを、秘密鍵を用いて復号し、前記第 1 メッセージと前記第 2 メッセージとが一致するか否かに基づいて、前記通信デバイスの認証を行っても良い。

[0020] (9) 本発明の第 1 の態様において、前記通信デバイスは、前記第 1 証明書を保持しなくても良い。

[0021] (10) 本発明の第 1 の態様において、前記データベースが格納する前記第 1 証明書には、公開鍵が含まれ、前記公開鍵に対応する秘密鍵は、前記通信デバイスによって保持されても良い。

[0022] (11) 本発明の第 1 の態様において、前記第 1 証明書には、有効期限が設定され、前記有効期限が切れる前に、前記データベースは、新たな有効期限が設定された前記第 1 証明書に更新しても良い。

[0023] (12) 本発明の第 1 の態様において、前記管理装置は、チャレンジ・レスポンス方式を用いて、前記通信デバイスの認証を行っても良い。

[0024] (13) 本発明の第 1 の態様において、前記通信デバイスの認証に成功した場合に、前記管理装置は、前記通信デバイスからの前記接続要求を受け入れ、前記通信デバイスを前記第 1 ネットワークに接続しても良い。

[0025] (14) 本発明の第 1 の態様において、前記通信デバイスの認証に成功しなかった場合に、前記管理装置は、前記制御部は、前記通信デバイスからの前記接続要求を拒否し、前記通信デバイスを、前記第 1 ネットワークに接続しなくても良い。

[0026] (15) 本発明の第 1 の態様において、前記管理装置は、前記通信デバイスから前記第 1 証明書を受信しなくても良い。

- [0027] (16) 本発明の第1の態様において、前記管理装置は、前記通信デバイスからの接続要求として、匿名接続要求を受信して、前記通信デバイスを、前記第1ネットワークに匿名接続させ、前記通信デバイスの認証に成功した場合に、前記管理装置は、前記通信デバイスを、匿名接続から正規接続に切り替えて、前記第1ネットワークに接続させても良い。
- [0028] (17) 本発明の第1の態様において、前記通信デバイスの認証に成功しなかった場合に、前記管理装置は、前記通信デバイスの匿名接続を、前記第1ネットワークから切断しても良い。
- [0029] (18) 本発明の第1の態様において、前記通信デバイスからの接続要求を受信した場合に、前記管理装置は、前記第1証明書を前記第2証明書を用いて検証しても良い。
- [0030] (19) 本発明の第2の態様は、ネットワークに接続される通信デバイスからの接続要求を受信する通信部と、前記通信部が前記接続要求を受信した場合に、前記接続要求を行った前記通信デバイスを認証するための第1証明書を、データベースから読み出す制御部と、前記制御部が読み出した前記第1証明書を用いて、前記接続要求を送信した前記通信デバイスの認証を行う認証部と、を備える管理装置である。
- [0031] (20) 本発明の第3の態様は、ネットワークに接続される通信デバイスからの接続要求を受信し、前記接続要求を受信した場合に、前記通信デバイスを認証するために用いられる第1証明書を格納するデータベースから、前記接続要求を行った前記通信デバイスを認証するための第1証明書を読み出し、読み出した前記第1証明書を用いて、前記接続要求を行った前記通信デバイスの認証を行う認証方法である。

発明の効果

- [0032] 本発明の一態様によれば、通信デバイスからの接続要求があった場合に、その接続要求を行った通信デバイスを認証するための第1証明書をデータベースから読み出し、読み出した第1証明書を用いて接続要求を行った通信デバイスの認証を行う。このため、通信デバイスを認証するための第1証明書

の管理はデータベースに格納されたものを管理すれば良いため、通信デバイスの認証に用いられる証明書の管理を簡素化することができる。また、接続要求を行った通信デバイスとの間で証明書の送受信は行われなため、証明書の送受信に要するリソースを削減することができる。

図面の簡単な説明

[0033] [図1]本発明の第1実施形態による認証システムの全体構成を示すブロック図である。

[図2]本発明の第1実施形態で用いられるPKIを説明するための図である。

[図3]本発明の第1実施形態における証明書の組み込み方法の一例を示す図である。

[図4]本発明の第1実施形態による認証システムの第1動作を示すフローチャートである。

[図5]本発明の第1実施形態による認証システムの第1動作を示すタイミングチャートである。

[図6]本発明の第1実施形態による認証システムの第2動作を示すフローチャートである。

[図7]本発明の第1実施形態による認証システムの第2動作を示すタイミングチャートである。

[図8]本発明の第2実施形態による認証システムの全体構成を示すブロック図である。

[図9]本発明の第3実施形態で用いられるPKIを説明するための図である。

[図10]本発明の第4実施形態による認証システムの動作を示すフローチャートである。

発明を実施するための形態

[0034] 以下、図面を参照して本発明の第1～第4実施形態による認証システム、管理装置及び認証方法について詳細に説明する。

[0035] [第1実施形態]

図1は、本発明の第1実施形態による認証システム1の全体構成を示すブ

ロック図である。図 1 に示す通り、第 1 実施形態の認証システム 1 は、無線デバイス 10 a ~ 10 c（通信デバイス）、無線ルータ 20 a, 20 b、バックボーンルータ 30、システムマネージャ 40 a（管理装置）、及び認証データベース 50（データベース）を備える。システムマネージャ 40 a は、認証データベース 50 を用いて無線ネットワーク N 1（ネットワーク）に接続される無線デバイス 10 a ~ 10 c の認証を行う。尚、図 1 に示す無線デバイス 10 a ~ 10 c 及び無線ルータ 20 a, 20 b の数は任意である。

[0036] 図 1 中の無線ネットワーク N 1 は、システムマネージャ 40 a の管理制御の下で、無線デバイス 10 a ~ 10 c、無線ルータ 20 a, 20 b、及びバックボーンルータ 30 によって形成される。無線ネットワーク N 1 は、省電力で低速（通信帯域が所定値よりも狭い）であるという特質を有する無線のネットワークである。また、バックボーンルータ 30 及びシステムマネージャ 40 a が接続されるバックボーンネットワーク N 2 は、広帯域（通信帯域が所定値よりも広い）であるという特質を有する認証システム 1 の基幹となる有線又は無線のネットワークである。

[0037] 無線デバイス 10 a ~ 10 c は、例えば流量計や温度センサ等のセンサ機器、流量制御弁や開閉弁等のバルブ機器、ファンやモータ等のアクチュエータ機器等のプラントや工場に設置される無線フィールド機器である。これら無線デバイス 10 a ~ 10 c は、電池を電源として間欠動作を行い、インダストリアル・オートメーション用無線通信規格である I S A 1 0 0 . 1 1 a に準拠した無線通信を行う。

[0038] ここで、無線デバイス 10 a ~ 10 c は、システムマネージャ 40 a によって認証されなければ正規に無線ネットワーク N 1 に接続することができない。このため、これら無線デバイス 10 a ~ 10 c には、自身が正規の無線デバイスであることを示す証明書 C 1 1 ~ C 1 3（図 2 参照）がそれぞれ予め用意される。詳細は後述するが、証明書 C 1 1 ~ C 1 3 は、認証データベース 50 に格納されるため、必ずしも無線デバイス 10 a ~ 10 c に保持される必要は無い。

- [0039] 無線ルータ 20a, 20b は、無線デバイス 10a~10c 及びバックボーンルータ 30 との間で無線通信規格 I S A 1 0 0 . 1 1 a に準拠した無線通信を行う。つまり、無線ルータ 20a, 20b は、無線デバイス 10a~10c とバックボーンルータ 30 との間で送受信されるデータを中継する。これら無線ルータ 20a, 20b も、無線デバイス 10a~10c と同様に、電池を電源として間欠動作を行う。上記の無線デバイス 10a~10c、無線ルータ 20a, 20b、及びバックボーンルータ 30 が互いに無線接続されることにより、スター・メッシュ状の無線ネットワーク N 1 が形成される。尚、無線ルータ 20a, 20b に代えて、無線ルータ 20a, 20b の機能（中継機能）を備える無線デバイスが設けられても良い。
- [0040] バックボーンルータ 30 は、無線ネットワーク N 1 とバックボーンネットワーク N 2 とを接続し、無線デバイス 10a~10c 等とシステムマネージャ 40a との間で送受信される各種データの中継を行う。このバックボーンルータ 30 は、例えばバックボーンネットワーク N 2 から供給される直流電力、或いはバックボーンネットワーク N 2 とは別の経路を介して供給される直流電力により連続して動作する。バックボーンルータ 30 は、上記の無線通信規格 I S A 1 0 0 . 1 1 a に準拠した無線通信を行う。
- [0041] システムマネージャ 40a は、例えば商用電源から供給される電力により連続して動作し、認証システム 1 を統括して管理制御する。例えば、システムマネージャ 40a は、無線ネットワーク N 1 を介して行われる無線通信の制御を行う。具体的には、システムマネージャ 40a は、無線デバイス 10a~10c、無線ルータ 20a, 20b、及びバックボーンルータ 30 に対する無線通信リソース（タイムスロット及び通信チャネル）の割り当て制御を行う。これにより、システムマネージャ 40a は、無線ネットワーク N 1 を介した T D M A（Time Division Multiple Access：時分割多元接続）による無線通信を実現する。
- [0042] また、システムマネージャ 40a は、認証データベース 50 に格納された証明書 C 1 1 ~ C 1 3 及び証明書 C 2 0（図 2 参照）を用いて無線ネットワ

ークN 1 に接続される無線デバイス1 0 a～1 0 cの認証を行う。具体的に、システムマネージャ4 0 aは、無線デバイス1 0 a～1 0 cからの接続要求があった場合に、認証データベース5 0 に格納された証明書C 1 1～C 1 3（図2 参照）を、証明書C 2 0（図2 参照）を用いて検証する。その後、システムマネージャ4 0 aは、チャレンジ・レスポンス方式により接続要求を行った無線デバイス1 0 a～1 0 cの認証を行う。

図1 に示すように、システムマネージャ4 0 aは、通信部4 1、制御部4 2 a、認証部4 3を備える。

通信部4 1は、無線ネットワークN 1 に接続される無線デバイス1 0 a～1 0 cからの接続要求を、それぞれ受信する。

制御部4 2 aは、通信部4 1が接続要求を受信した場合に、接続要求を行った無線デバイス（例えば、無線デバイス1 0 a）を認証するための証明書（例えば、証明書C 1 1）を、認証データベース5 0 から読み出す。

認証部4 3は、制御部4 2 aが読み出した証明書（例えば、証明書C 1 1）を用いて、接続要求を送信した無線デバイス（例えば、無線デバイス1 0 a）の認証を行う。

[0043] 認証データベース5 0は、無線デバイス1 0 a～1 0 cの認証を行うために必要な情報が格納されるデータベースである。具体的に、認証データベース5 0には、証明書C 1 1～C 1 3（第1 証明書：図2 参照）と、証明書C 2 0（第2 証明書：図2 参照）とが格納される。証明書C 1 1～C 1 3は、無線デバイス1 0 a～1 0 cについての証明書である。証明書C 2 0は、信頼できる認証局によって発行された証明書であって、証明書C 1 1～C 1 3を検証するために用いられる証明書C 2 0（第2 証明書：図2 参照）である。尚、無線デバイス1 0 a～1 0 cについての証明書C 1 1～C 1 3は、無線デバイス1 0 a～1 0 cを一意に特定する識別子（例えば、E U I 6 4 アドレス）に対応付けられて認証データベース5 0 に格納される。

[0044] 無線デバイス1 0 a～1 0 cについての証明書C 1 1～C 1 3は、本来であれば無線デバイス1 0 a～1 0 cにそれぞれ保持される。しかし、第1 実

施形態では、証明書C 1 1～C 1 3は、認証データベース5 0に格納され、無線デバイス1 0 a～1 0 cでは保持されない。これは、無線デバイス1 0 a～1 0 cについての証明書の管理を簡素化するためである。また、無線ネットワークN 1を介した証明書C 1 1～C 1 3の送受信を無くすことによって、証明書C 1 1～C 1 3の送受信のために必要となるリソースを削減するためである。

[0045] 図2は、本発明の第1実施形態で用いられるPKI (Public Key Infrastructure: 公開鍵基盤)を説明するための図である。図2に示す通り、無線デバイス1 0 a～1 0 cについての証明書C 1 1～C 1 3、及びこれら証明書C 1 1～C 1 3を検証するために用いられる証明書C 2 0は、認証局6 0に、システムマネージャ4 0 aが発行を要求する(P 1 1)。この要求に対して、認証局6 0は、システムマネージャ4 0 aに、証明書C 1 1～C 1 3、証明書C 2 0を発行する(P 1 2)。認証局6 0は、システムマネージャ4 0 aが信頼できる認証局であり、例えば、公的な認証局である。この認証局6 0によって発行された証明書C 1 1～C 1 3及び証明書C 2 0は、認証データベース5 0に格納される。尚、無線デバイス1 0 a～1 0 cについての証明書C 1 1～C 1 3は、認証データベース5 0に格納されるとともに、無線デバイス1 0 a～1 0 cにそれぞれ保持されても良い。この場合には、例えば、証明書C 1 1は、認証局6 0から無線デバイス1 0 aに送信される(P 1 3)。

[0046] 図2では図示を省略しているが、証明書C 1 1～C 1 3及び証明書C 2 0にはそれぞれ異なる公開鍵が含まれる。証明書C 1 1～C 1 3に含まれている公開鍵に対応する秘密鍵は、無線デバイス1 0 a～1 0 cにそれぞれ保持される。証明書C 2 0に含まれている公開鍵に対応する秘密鍵は、認証局6 0に保持されて厳重に管理される。

[0047] 無線ネットワークN 1に対する接続要求が無線デバイス1 0 aからあった場合には、図2に示す通り、認証データベース5 0に格納された証明書C 1 1と証明書2 0とを用いた無線デバイス1 0 aの認証がシステムマネージャ

40aによって行われる（P14）。尚、無線ネットワークN1に対する接続要求が無線デバイス10bからあった場合には、認証データベース50に格納された証明書C12と証明書20とを用いて無線デバイス10bの認証が行われる。また、無線ネットワークN1に対する接続要求が無線デバイス10cからあった場合には、認証データベース50に格納された証明書C13と証明書20とを用いて無線デバイス10cの認証が行われる。

[0048] 次に、認証局60によって発行される証明書C11～C13及び証明書C20の組み込み方法について説明する。図3は、本発明の第1実施形態における証明書C11～C13の組み込み方法の一例を示す図である。プラントや工場で実現される無線ネットワークN1は、インターネット等の一般的なネットワークとは異なる。無線ネットワークN1は、無線ネットワークN1を構成する機器（無線デバイス10a～10c、無線ルータ20a、20b、及びバックボーンルータ30）の設置場所、数、種類等が綿密に計画されて設計される。このため、無線ネットワークN1の設計が終了した段階で、無線ネットワークN1に接続させる必要のある無線デバイスが確定し、その認証に必要な証明書も確定する。

[0049] 無線ネットワークN1の設計が終了すると、無線デバイスのベンダVは、認証局60に対し、無線ネットワークN1に接続させる必要のある無線デバイス10a～10cについての証明書C11～C13及び証明書C20の発行を要求する。これに対して、認証局60は、無線デバイス10a～10cについての証明書C11～C13及び証明書C20を発行する（P21）。認証局60から発行された証明書C11～C13及び証明書C20を取得すると、ベンダVは、証明書C11～C13を無線デバイス10a～10cにそれぞれ組み込む（P22）。それとともに、ベンダVは、証明書C11～C13及び証明書C20をCD-ROM又はDVD（登録商標）-ROM等のコンピュータ読み取り可能な記録媒体Mにコピーする（P23）。そして、ベンダVは、証明書の組み込みを終えた無線デバイス（図3に示す例では、無線デバイス10a）を、ユーザU（例えば、プラントや工場で認証シス

テム１の運用を行っている者）に発送する（Ｐ２４）。また、ベンダＶは、証明書Ｃ１１～Ｃ１３及び証明書Ｃ２０が記録された記録媒体Ｍを、ユーザＵに発送する（Ｐ２５）。

[0050] ユーザＵは、ベンダＶから発送されてきた無線デバイス１０ａを、設計段階で規定された位置に設置し、ベンダＶから発送されてきた記録媒体Ｍに記録された証明書Ｃ１１～Ｃ１３及び証明書Ｃ２０をシステムマネージャ４０ａに組み込む（Ｐ２６）。証明書Ｃ２０は認証システム１の信頼性を保つための基礎となるデータであるため、証明書Ｃ２０は、安全な方法を用いてインテグリティ（完全性）が確認され、システムマネージャ４０ａに組み込まれる。尚、システムマネージャ４０ａに組み込まれた証明書Ｃ１１～Ｃ１３は、無線デバイス１０ａ～１０ｃを一意に特定する識別子に対応付けられて認証データベース５０に格納される。システムマネージャ４０ａに組み込まれた証明書Ｃ２０は、単独で認証データベース５０に格納される。このようにして、認証データベース５０に対する証明書Ｃ１１～Ｃ１３及び証明書Ｃ２０の組み込みが行われる。

[0051] ここで、ユーザＵが無線ネットワークＮ１のネットワーク設計書ＮＤを参照してベンダＶに依頼すれば（Ｐ２７）、無線ネットワークＮ１に接続させようとしている無線デバイスの証明書であって、認証データベース５０に格納されていないものを取得することが可能である。

また、証明書Ｃ１１～Ｃ１３に有効期限が設定される場合には、その有効期限が切れる前に、ユーザＵがベンダＶに依頼して新たな有効期限が設定された証明書Ｃ１１～Ｃ１３或いは証明書Ｃ２０を取得すれば、認証データベース５０に格納された証明書Ｃ１１～Ｃ１３或いは証明書Ｃ２０を更新することも可能である。尚、証明書Ｃ１１～Ｃ１３及び証明書Ｃ２０は、公開しても良いため、ユーザＵがベンダＶから記録媒体Ｍを入手する経路は適宜選択することができる。

[0052] 次に、上記構成における認証システム１の動作について説明する。尚、以下では、無線ネットワークＮ１に接続させようとしている無線デバイスが無

線デバイス 10a である場合について説明する。そして、この無線デバイス 10a の認証を行う場合の動作を例に挙げて説明する。ここで、認証システム 1 の動作は、ピギーバック (PiggyBack) 方式に準じた方法で証明書が提示される際の動作 (第 1 動作) と、匿名接続法によって証明書が提示される際の動作 (第 2 動作) とに大別される。以下では、これら第 1, 第 2 動作について順に説明する。

[0053] <第 1 動作>

図 4 は、本発明の第 1 実施形態による認証システム 1 の第 1 動作を示すフローチャートである。図 5 は、認証システム 1 の第 1 動作を示すタイミングチャートである。図 4, 図 5 に示す通り、まず無線デバイス 10a を認証するために用いられる証明書を準備するオフライン時の動作が行われる (ステップ S 10)。次にオフライン時に準備された証明書を用いて無線デバイス 10a の認証を行うオンライン時の動作が行われる (ステップ S 20)。

[0054] オフライン時の動作が開始されると、まず認証局 60 が発行した証明書 C 20 を取得して認証データベース 50 に格納する処理がシステムマネージャ 40a の制御部 42a で行われる (ステップ S 11)。例えば、図 3 を用いて説明した記録媒体 M (ベンダ V から発送された記録媒体 M) に記録された証明書 C 20 をシステムマネージャ 40a の制御部 42a が読み出して、認証データベース 50 に格納する処理が行われる。

[0055] 次に、認証局 60 が発行した証明書 C 11 ~ C 13 を取得し、これら証明書 C 11 ~ C 13 の正当性を、証明書 C 20 を用いて検証する処理がシステムマネージャ 40a の制御部 42a で行われる (ステップ S 12)。例えば、図 3 を用いて説明した記録媒体 M (ベンダ V から発送された記録媒体 M) に記録された証明書 C 11 ~ C 13 を読み出すとともに、ステップ S 11 の処理で認証データベース 50 に格納した証明書 C 20 を読み出し、証明書 C 11 ~ C 13 の正当性を、証明書 C 20 を用いて検証する処理がシステムマネージャ 40a の制御部 42a で行われる。

[0056] 次いで、証明書 C 11 ~ C 13 が正当であるか否かがシステムマネージャ

40aの制御部42aで判定される（ステップS13）。仮に、証明書C11～C13が不当であるとシステムマネージャ40aの制御部42aが判定した場合（判定結果が「NO」の場合）には、図4に示す一連の処理は終了する。これに対し、証明書C11～C13が正当であるとシステムマネージャ40aの制御部42aが判定した場合（判定結果が「YES」の場合）には、無線デバイス10a～10cを一意に特定する識別子に対応付けて証明書C11～C13を認証データベース50に格納する処理が制御部42aにより行われる（ステップS14）。以上の処理が終了すると、オフライン時の動作が終了し、オンライン時の動作が開始される。

[0057] オンライン時の動作が開始されると、システムマネージャ40aは、制御部42aの制御に基づいて、無線ネットワークN1を介した接続要求の受信待ち状態になる（ステップS21）。かかる状態のときに、無線ネットワークN1に対する接続要求が無線デバイス10aから送信されると、この接続要求はシステムマネージャ40aの通信部41で受信される（ステップS22）。

ここで、本来のピギーバック法であれば、接続要求とともに無線デバイス10aについての証明書が無線デバイス10aからシステムマネージャ40aに送信されるが、第1実施形態では証明書は送付されずに接続要求のみが送信される。このため、システムマネージャ22の通信部41では、無線デバイス10aの接続要求のみが受信される。

[0058] 無線デバイス10aからの接続要求を通信部41が受信すると、システムマネージャ40aの制御部42aは、無線デバイス10aの識別子に対応付けられた証明書C11を認証データベース50から読み出す（ステップS23）。尚、認証データベース50を検索する際に用いられる無線デバイス10aの識別子は、接続要求に付随して無線デバイス10aから送信される。

[0059] 無線デバイス10aについての証明書C11を制御部42aが読み出すと、システムマネージャ40aの認証部43は、チャレンジ・レスポンス方式により無線デバイス10aとの間でデータ（メッセージ）の送受信を行って

無線デバイス 10a の認証を行う（ステップ S24）。

具体的には、まず、システムマネージャ 40a の認証部 43 が、ステップ S23 で認証データベース 50 から読み出した証明書 C11 に含まれる公開鍵を用いて特殊なメッセージを暗号化し、この暗号化したメッセージを、通信部 41 が、無線ネットワーク N1 を介して無線デバイス 10a に対して送信する（チャレンジ）。

[0060] システムマネージャ 40a の通信部 41 から送信されたメッセージを受信すると、無線デバイス 10a は、自身が保持している秘密鍵を用いてメッセージを復号する。尚、システムマネージャ 40a からのメッセージは、無線デバイス 10a についての証明書 C11 に含まれる公開鍵を用いて暗号化されているため、無線デバイス 10a に保持されている秘密鍵のみで復号することができる。

[0061] システムマネージャ 40a からのメッセージを復号すると、無線デバイス 10a は、復号したメッセージをセキュアな方法でシステムマネージャ 40a に提示する（レスポンス）。

例えば、無線デバイス 10a は、システムマネージャ 40a の公開鍵を用いてメッセージ（復号したメッセージ）を暗号化し、暗号化したメッセージをシステムマネージャ 40a に向けて送信する。

[0062] 尚、無線デバイス 10a からシステムマネージャ 40a に送信されたメッセージは、システムマネージャ 40a に保持されて管理されている秘密鍵のみで復号することができる。そのため、無線デバイス 10a は、復号したメッセージをセキュアな方法でシステムマネージャ 40a に提示することができる。或いは、無線デバイス 10a が、復号したメッセージの一部を対象鍵とみなし、その鍵によって、復号したメッセージ又はメッセージの一部を暗号処理することで、セキュアな方法でシステムマネージャ 40a に提示することができる。

[0063] 無線デバイス 10a から提示されたメッセージを通信部 41 が受信すると、システムマネージャ 40a の認証部 43 は、無線デバイス 10a に送信し

たメッセージの内容から無線デバイス10aの認証に成功したか否かを判定する（ステップS25）。具体的には、無線デバイス10aに送信したメッセージと無線デバイス10aから提示されたメッセージとが事前に定義された一定の検証ルールに従って一致するか否かによって、無線デバイス10aの認証に成功したか否かを認証部43は判定する。

[0064] 認証に成功したと認証部43が判定した場合（ステップS25の判定結果が「YES」の場合）には、システムマネージャ40aの制御部42aは、無線デバイス10aからの接続要求を受け入れ、通信部41は、認証に成功した旨を示す認証結果を無線デバイス10aに通知する（ステップS26）。以上の処理によって、無線デバイス10aは、正規に無線ネットワークN1に接続され、システムマネージャ40aの管理の下で無線ネットワークN1を介した通信が可能になる。

[0065] これに対し、認証に失敗したと認証部43が判定した場合（ステップS25の判定結果が「NO」の場合）には、システムマネージャ40aの制御部42aは、無線デバイス10aからの接続要求を拒否し、通信部41は、認証に失敗した旨を示す認証結果を無線デバイス10aに通知する（ステップS27）。

以上の処理によって、無線デバイス10aの無線ネットワークN1に対する接続要求は拒否されるため、無線デバイス10aは、無線ネットワークN1に接続されず、無線ネットワークN1を介した通信を行うことができない。

[0066] 〈第2動作〉

図6は、本発明の第1実施形態による認証システム1の第2動作を示すフローチャートである。図7は、認証システム1の第2動作を示すタイミングチャートである。尚、図6、図7においては、図4、図5に示した処理と同様の処理が行われるステップには同一の符号を付してある。図6、図7に示す通り、第2動作においても、最初にオフライン時の動作が行われ（ステップS10）、続いてオンライン時の動作が行われる（ステップS20）。但

し、第2動作におけるオフライン時の動作は第1動作におけるオフライン時の動作と同様であるため、以下ではオフライン時の動作の説明を省略し、オンライン時の動作についてのみ説明する。

[0067] オンライン時の動作が開始されると、システムマネージャ40aは、制御部42aの制御に基づいて、無線ネットワークN1を介した接続要求の受信待ち状態になる（ステップS21）。かかる状態のときに、無線ネットワークN1に対する匿名接続要求が無線デバイス10aから送信されると、この匿名接続要求はシステムマネージャ40aの通信部41で受信されて受け入れられ、制御部42aの制御に基づいて、無線デバイス10aとシステムマネージャ40aとの間で匿名接続が確立される（ステップS31）。尚、ここでは、従来の匿名接続法と同様に、無線デバイス10aからシステムマネージャ40aに対する証明書の送付は行われない。

[0068] 無線デバイス10aとの間の匿名接続が制御部42aにより確立されると、システムマネージャ40aの制御部42aは、無線デバイス10aの識別子に対応付けられた証明書C11を認証データベース50から読み出す（ステップS23）。尚、認証データベース50を検索する際に用いられる無線デバイス10aの識別子は、匿名接続要求に付随して無線デバイス10aから送信され、通信部41により受信される。

[0069] 無線デバイス10aについての証明書C11を制御部42aが読み出すと、システムマネージャ40aの制御部42aは、チャレンジ・レスポンス方式により無線デバイス10aとの間でデータ（メッセージ）の送受信を通信部41を介して行って、無線デバイス10aの認証を認証部43により行う（ステップS24）。尚、チャレンジ・レスポンス方式による無線デバイス10aの認証は、第1動作と同様の処理により行われるため、ここでの詳細な説明は省略する。

[0070] 次いで、システムマネージャ40aは、無線デバイス10aの認証に成功したか否かを認証部43は判定する（ステップS25）。認証に成功したと認証部43が判定した場合（判定結果が「YES」の場合）には、システム

マネージャ 40a の制御部 42a は、無線デバイス 10a との間で確立されている匿名接続を正規な接続に切り替える処理を行う（ステップ S32）。以上の処理によって、無線デバイス 10a は、正規に無線ネットワーク N1 に接続され、システムマネージャ 40a の管理の下で無線ネットワーク N1 を介した通信が可能になる。

[0071] これに対し、認証に失敗したと認証部 43 が判定した場合（ステップ S25 の判定結果が「NO」の場合）には、システムマネージャ 40a の制御部 42a は、無線デバイス 10a との間の匿名接続を切断する処理を行う（ステップ S33）。以上の処理によって、無線デバイス 10a は無線ネットワーク N1 から切り離されるため、無線ネットワーク N1 を介した通信を行うことができなくなる。

[0072] 以上説明した通り、第 1 実施形態では、無線デバイス 10a～10c についての証明書 C11～C13（証明書 C20 を用いて検証されたもの）を格納する認証データベース 50 を設ける。そして、無線デバイス 10a からの接続要求又は匿名接続要求を通信部 41 が受信した場合には、システムマネージャ 40a の制御部 42a が、無線デバイス 10a についての証明書 C11 を認証データベース 50 から読み出して、認証部 43 が無線デバイス 10a の認証を行う。

[0073] これにより、無線デバイス 10a～10c についての証明書 C11～C13 の管理は、認証データベース 50 に格納されたものについて行えば良く、無線デバイス 10a～10c に保持されるものについては行う必要がなくなる。そのため、証明書 C11～C13 の管理を簡素化することができる。また、前述した第 1、第 2 動作の何れの動作が行われる場合であっても、無線ネットワーク N1 を介して証明書 C11～C13 が送受信されることがなくなる。そのため、証明書 C11～C13 の送受信に要するリソースを削減することができる。

[0074] [第 2 実施形態]

図 8 は、本発明の第 2 実施形態による認証システム 2 の全体構成を示すブ

ロック図である。尚、図8においては、図1に示した構成と同様の構成については同一の符号を付してある。図8に示す通り、第2実施形態の認証システム2は、認証データベース50に格納されている証明書を提供する認証サーバ70（サーバ装置）を設け、システムマネージャ40bと認証サーバ70とをLAN（Local Area Network）等のネットワークN3で接続した構成である。

第2実施形態では、システムマネージャ40bは、第1実施形態のシステムマネージャ40aと異なり、制御部42aの代わりに制御部42bを備える。

[0075] 前述した第1実施形態の認証システム1では、システムマネージャ40aが認証データベース50に直接接続されており、システムマネージャ40aが、認証データベース50からの証明書C11～C13の読み出しを行っていた。これに対し、第2実施形態の認証システム2では、システムマネージャ40bの制御部42bは、認証サーバ70に対して証明書C11～C13の読み出し要求を行い、要求に応じた証明書C11～C13が認証サーバ70によって制御部42bに提供される。尚、システムマネージャ40bが、証明書C11～C13の読み出し要求を行う場合には、無線デバイス10a～10cを一意に特定する識別子を認証サーバ70に提供する必要がある。

[0076] 以上の通り、第2実施形態では、認証データベース50に格納されている証明書を提供する認証サーバ70を設けているため、システムマネージャ40bの負荷を低減することができる。尚、図8では、1つの認証サーバ70がネットワークN3を介してシステムマネージャ40bに接続されている構成を例示しているが、複数の認証サーバ70がネットワークN3を介してシステムマネージャ40bに接続されている構成であっても良い。また、認証サーバ70は、バックボーンネットワークN2を介してシステムマネージャ40bに接続されていても良い。

[0077] [第3実施形態]

次に、本発明の第3実施形態について説明する。前述した第1及び第2実

施形態では、システムマネージャ 40a 及び 40b が信頼できる認証局 60（例えば、公的な認証局）が発行した証明書 C11～C13 及び証明書 C20 を用いて無線デバイス 10a～10c の認証を行っていた。これに対し、第 3 実施形態では、ユーザ U が独自に構築した認証局が発行した証明書を用いて無線デバイス 10a～10c の認証を行う（P33）。

第 3 実施形態では、システムマネージャ 40c は、第 1 実施形態のシステムマネージャ 40a と異なり、制御部 42a の代わりに制御部 42c を備える。

[0078] 図 9 は、本発明の第 3 実施形態で用いられる PKI を説明するための図である。図 9 に示す通り、第 3 実施形態では、ユーザ U が独自に構築した認証局である認証局サーバ装置 80 が設けられる。この認証局サーバ装置 80 は、無線デバイス 10a～10c の認証を行うために用いられる証明書 C31～C33（第 1 証明書）、及びこれらの証明書 C31～C33 を検証するために用いられる証明書 C20 を発行する（P32）。尚、認証局サーバ装置 80 は、例えば図 8 に示す認証システム 2 に設けられるネットワーク N3 に接続されていても良いが、セキュリティを向上させるために認証システム 2 とは分離されても良い。

[0079] 認証局サーバ装置 80 が新たに発行した証明書 C31～C33 及び証明書 C20 は、認証データベース 50 に格納され、システムマネージャ 40c によって証明書 C31～C33 及び証明書 C20 を用いた無線デバイス 10a～10c の認証が行われる。しかしながら、無線デバイス 10a～10c に格納された秘密鍵を更新することは容易ではない。

[0080] そこで、図 9 に示す通り、システムマネージャ 40c が認証データベース 50 から、例えば無線デバイス 10a に対応した証明書 C11 を、制御部 42c が取り出し、そこに含まれる公開鍵を提示して認証局サーバ装置 80 に署名要求を行う（P31）。このような認証局サーバ装置 80 を設ければ、ユーザ U が独自に構築した認証局を用いて、これまでに述べたような PKI を用いた無線デバイスの認証が可能となる。また、こうして生成した証明書

C 3 1 を無線デバイス 1 0 a にシステムマネージャ 4 0 c を介して組み込んでも良い。尚、無線デバイス 1 0 a ~ 1 0 c が、秘密鍵を設定するインターフェイスを提供している場合、図 3 のベンダ V が行ったように認証局サーバ装置 8 0 が秘密鍵とペアになる公開鍵を含む証明書を作成し、システムマネージャ 4 0 c を介して、それらを組み込んでも良い。

[0081] [第 4 実施形態]

次に、本発明の第 4 実施形態について説明する。前述した第 1 及び第 2 実施形態では、システムマネージャ 4 0 a 及び 4 0 b が認証データベース 5 0 に格納された証明書 C 1 1 ~ C 1 3 を用いて無線デバイス 1 0 a ~ 1 0 c の認証を行っていた。第 4 実施形態では、無線デバイス 1 0 a ~ 1 0 c の認証を行うための証明書 C 1 1 ~ C 1 3 が認証データベース 5 0 に格納されていない場合にも、無線デバイス 1 0 a ~ 1 0 c に保持されている証明書 C 1 1 ~ C 1 3 を取得することにより、無線デバイス 1 0 a ~ 1 0 c の認証を可能とする（フォールバック）。

なお、第 4 実施形態の認証システムの構成については、図 1 に示される第 1 実施形態の認証システム 1 の構成と同様であるため、それらの構成を引用して説明する。

[0082] このため、第 4 実施形態では、有効期限が経過していない証明書 C 1 1 ~ C 1 3 が無線デバイス 1 0 a ~ 1 0 c に保持されていることが前提となる。尚、第 4 実施形態による認証システムの全体構成は、図 1 に示す第 1 実施形態による認証システム 1 或いは図 8 に示す第 2 実施形態による認証システム 2 と同様である。

[0083] 図 1 0 は、本発明の第 4 実施形態による認証システムの動作を示すフローチャートである。この図 1 0 に示すフローチャートは、図 6 に示すフローチャートと同様に、匿名接続法によって証明書が提示される際の動作（第 2 動作）を示す。尚、図 1 0 においては、オフライン時の動作（ステップ S 1 0）を省略し、オンライン時の動作（ステップ S 2 0）のみを図示している。尚、図 1 0 においては、図 6 に示した処理と同様の処理が行われるステップ

には同一の符号を付してある。

[0084] オンライン時の動作が開始されると、システムマネージャ40aは、制御部42aの制御に基づいて、第1実施形態における第2動作と同様に、無線ネットワークN1を介した接続要求の受信待ち状態になる（ステップS21）。かかる状態のときに、無線ネットワークN1に対する匿名接続要求が無線デバイス10aから送信されると、この匿名接続要求はシステムマネージャ40aの通信部41で受信されて受け入れられ、制御部42aは、無線デバイス10aとシステムマネージャ40aとの間で匿名接続を確立する（ステップS31）。尚、ここでは、従来の匿名接続法と同様に、無線デバイス10aからシステムマネージャ40aに対する証明書の送付は行われない。

[0085] 無線デバイス10aとの間の匿名接続が確立されると、システムマネージャ40aの制御部42aは、無線デバイス10aの識別子に対応付けられた証明書C11を認証データベース50から読み出す（ステップS23）。尚、認証データベース50を検索する際に用いられる無線デバイス10aの識別子は、匿名接続要求に付随して無線デバイス10aから送信され、通信部41で受信される。

[0086] 次に、システムマネージャ40aの制御部42aは、認証データベース50からの証明書C11の読み出しに成功したか否かを判定する（ステップS41）。証明書C11の読み出しに成功したと制御部42aが判定した場合（判定結果が「YES」の場合）には、システムマネージャ40aの認証部43は、第1実施形態と同様に、チャレンジ・レスポンス方式により無線デバイス10aの認証を行う（ステップS24）。

[0087] これに対し、証明書C11の読み出しに失敗したと制御部42aが判定した場合（判定結果が「NO」の場合）には、システムマネージャ40aの認証部43は、無線デバイス10aに対して証明書C11の送信要求を通信部41を介して行い、通信部41は、無線デバイス10aから証明書C11を取得する（ステップS42）。

そして、無線デバイス10aから取得した証明書C11に含まれる公開鍵

を用いて、チャレンジ・レスポンス方式により無線デバイス10aの認証を認証部43は行う（ステップS24）。

[0088] 尚、無線デバイス10aの認証に認証部43が成功した場合には、第1実施形態と同様に、無線デバイス10aとの間で確立されている匿名接続を正規な接続に切り替える処理がシステムマネージャ40aの制御部42aによって行われる（ステップS32）。また、無線デバイス10aの認証に認証部43が失敗した場合には、第1実施形態と同様に、無線デバイス10aとの間の匿名接続を切断する処理がシステムマネージャ40aの制御部42aによって行われる（ステップS33）。

[0089] 以上説明した通り、第4実施形態では、無線デバイス10a～10cについての証明書C11～C13が認証データベース50に格納されていない場合には、無線デバイス10a～10cに保持された証明書C11～C13を取得して無線デバイス10a～10cの認証を認証部43が行う。このため、例えば認証データベース50に障害が生じた場合であっても、従来と同じ方法で無線デバイス10a～10cを無線ネットワークN1に接続させることができる。

[0090] 以上、本発明の第1～第4実施形態による認証システム、管理装置及び認証方法について説明したが、本発明は上述した第1～第4実施形態に制限されることなく、本発明の範囲内で自由に変更が可能である。例えば、上記第1～第4実施形態では、オフライン時（図4、図6中のステップS10）において、無線デバイス10a～10cの認証に用いられる証明書C11～C13を、証明書C20を用いて予め検証し、検証されたもののみを認証データベース50に格納するようにしていた。しかしながら、オフライン時における証明書C11～C13の検証（証明書C20を用いた検証）は行わず、オンライン時に無線デバイス10a～10cからの接続要求又は匿名接続要求を通信部41が受信したときに上記の検証を行うようにしても良い。

[0091] また、上記第1～第4実施形態では、バックボーンルータ30とシステムマネージャ40a、40b、40cとが別々に設けられる態様について説明

したが、本発明は、バックボーンルータ 30 とシステムマネージャ 40 a、40 b、40 c とが一体化されている態様であっても良い。かかる態様の場合には、バックボーンネットワーク N2 を省略することができる。また、上記第 1 ～第 4 実施形態では、無線ネットワーク N1 に接続される無線デバイス 10 a ～ 10 c を認証する例について説明したが、本発明は有線のネットワークに接続される通信デバイスの認証にも適用することができる。

産業上の利用可能性

[0092] 本発明は、通信デバイスの認証に用いられる証明書の管理を簡素化することが要求されるとともに、証明書の送受信に要するリソースを削減することが要求される認証システム、管理装置及び認証方法などに適用することができる。

符号の説明

[0093] 1, 2 認証システム
10 a ～ 10 c 無線デバイス
40 a、40 b、40 c システムマネージャ
41 通信部
42 a、42 b、42 c 制御部
43 認証部
50 認証データベース
70 認証サーバ
80 認証局サーバ装置
C11 ～ C13 証明書
C20 証明書
C31 ～ C33 証明書
N1 無線ネットワーク
N3 ネットワーク

請求の範囲

- [請求項1] 第1 ネットワークに接続される通信デバイスを認証するために用いられる第1 証明書を格納するデータベースと、
- 前記通信デバイスからの接続要求があった場合に、前記接続要求を行った前記通信デバイスを認証するための第1 証明書を前記データベースから読み出し、第1 証明書を用いて、前記接続要求を行った前記通信デバイスの認証を行う管理装置と、
- を備える認証システム。
- [請求項2] 前記データベースに格納される前記第1 証明書は、前記第1 証明書を検証するための第2 証明書を用いて検証される請求項1 記載の認証システム。
- [請求項3] 前記第1 ネットワークとは異なる第2 ネットワークを介して前記管理装置に接続され、前記データベースに格納された情報を提供するサーバ装置を更に備え、
- 前記管理装置は、前記サーバ装置から前記データベースに格納された前記第1 証明書を取得する請求項1 記載の認証システム。
- [請求項4] 前記データベースに格納される前記第1 証明書を発行する認証局サーバ装置を更に備える請求項1 記載の認証システム。
- [請求項5] 前記通信デバイスには、前記第1 証明書が付与されており、
- 前記管理装置は、前記接続要求を行った前記通信デバイスを認証するための前記第1 証明書が前記データベースに格納されていない場合には、前記接続要求を行った前記通信デバイスに付与されている前記第1 証明書を取得して、前記接続要求を行った前記通信デバイスの認証を行う請求項1 記載の認証システム。
- [請求項6] 前記第1 ネットワークは、無線ネットワークであり、
- 前記第2 ネットワークは、前記第1 ネットワークよりも通信帯域が広い請求項1 記載の認証システム。
- [請求項7] 前記データベースは、前記第1 証明書と、前記通信デバイスを一意

に特定する識別子とを対応付けて格納し、

前記管理装置は、

前記通信デバイスから、前記接続要求と、前記通信デバイスを一意に特定する識別子とを受信する通信部と、

前記通信部が受信した前記識別子に対応付けられた前記第 1 証明書を、前記データベースから読み出す制御部と、

前記制御部が読み出した前記第 1 証明書を用いて前記接続要求を行った前記通信デバイスの認証を行う制御部と、

を備える請求項 1 記載の認証システム。

[請求項 8] 前記認証部は、前記第 1 証明書に含まれる第 1 公開鍵を用いて第 1 メッセージを暗号化し、

前記通信部は、前記認証部が暗号化した前記第 1 メッセージを、前記通信デバイスに送信し、

前記通信部は、第 2 公開鍵を用いて暗号化された第 2 メッセージを、前記通信デバイスから受信し、

前記認証部は、前記第 2 メッセージを、秘密鍵を用いて復号し、前記第 1 メッセージと前記第 2 メッセージとが一致するか否かに基づいて、前記通信デバイスの認証を行う

請求項 7 記載の認証システム。

[請求項 9] 前記通信デバイスは、前記第 1 証明書を保持しない請求項 1 記載の認証システム。

[請求項 10] 前記データベースが格納する前記第 1 証明書には、公開鍵が含まれ、

前記公開鍵に対応する秘密鍵は、前記通信デバイスによって保持される請求項 1 記載の認証システム。

[請求項 11] 前記第 1 証明書には、有効期限が設定され、

前記有効期限が切れる前に、前記データベースは、新たな有効期限が設定された前記第 1 証明書に更新する請求項 1 記載の認証システム

。

[請求項12] 前記管理装置は、チャレンジ・レスポンス方式を用いて、前記通信デバイスの認証を行う請求項1記載の認証システム。

[請求項13] 前記通信デバイスの認証に成功した場合に、前記管理装置は、前記通信デバイスからの前記接続要求を受け入れ、前記通信デバイスを前記第1ネットワークに接続する請求項1記載の認証システム。

[請求項14] 前記通信デバイスの認証に成功しなかった場合に、前記管理装置は、前記制御部は、前記通信デバイスからの前記接続要求を拒否し、前記通信デバイスを、前記第1ネットワークに接続しない請求項13記載の認証システム。

[請求項15] 前記管理装置は、前記通信デバイスから前記第1証明書を受信しない請求項13記載の認証システム。

[請求項16] 前記管理装置は、前記通信デバイスからの接続要求として、匿名接続要求を受信して、前記通信デバイスを、前記第1ネットワークに匿名接続させ、

前記通信デバイスの認証に成功した場合に、前記管理装置は、前記通信デバイスを、匿名接続から正規接続に切り替えて、前記第1ネットワークに接続させる請求項1記載の認証システム。

[請求項17] 前記通信デバイスの認証に成功しなかった場合に、前記管理装置は、前記通信デバイスの匿名接続を、前記第1ネットワークから切断する請求項16記載の認証システム。

[請求項18] 前記通信デバイスからの接続要求を受信した場合に、前記管理装置は、前記第1証明書を前記第2証明書を用いて検証する請求項2記載の認証システム。

[請求項19] ネットワークに接続される通信デバイスからの接続要求を受信する通信部と、

前記通信部が前記接続要求を受信した場合に、前記接続要求を行った前記通信デバイスを認証するための第1証明書を、データベースか

ら読み出す制御部と、

前記制御部が読み出した前記第 1 証明書を用いて、前記接続要求を送信した前記通信デバイスの認証を行う認証部と、

を備える管理装置。

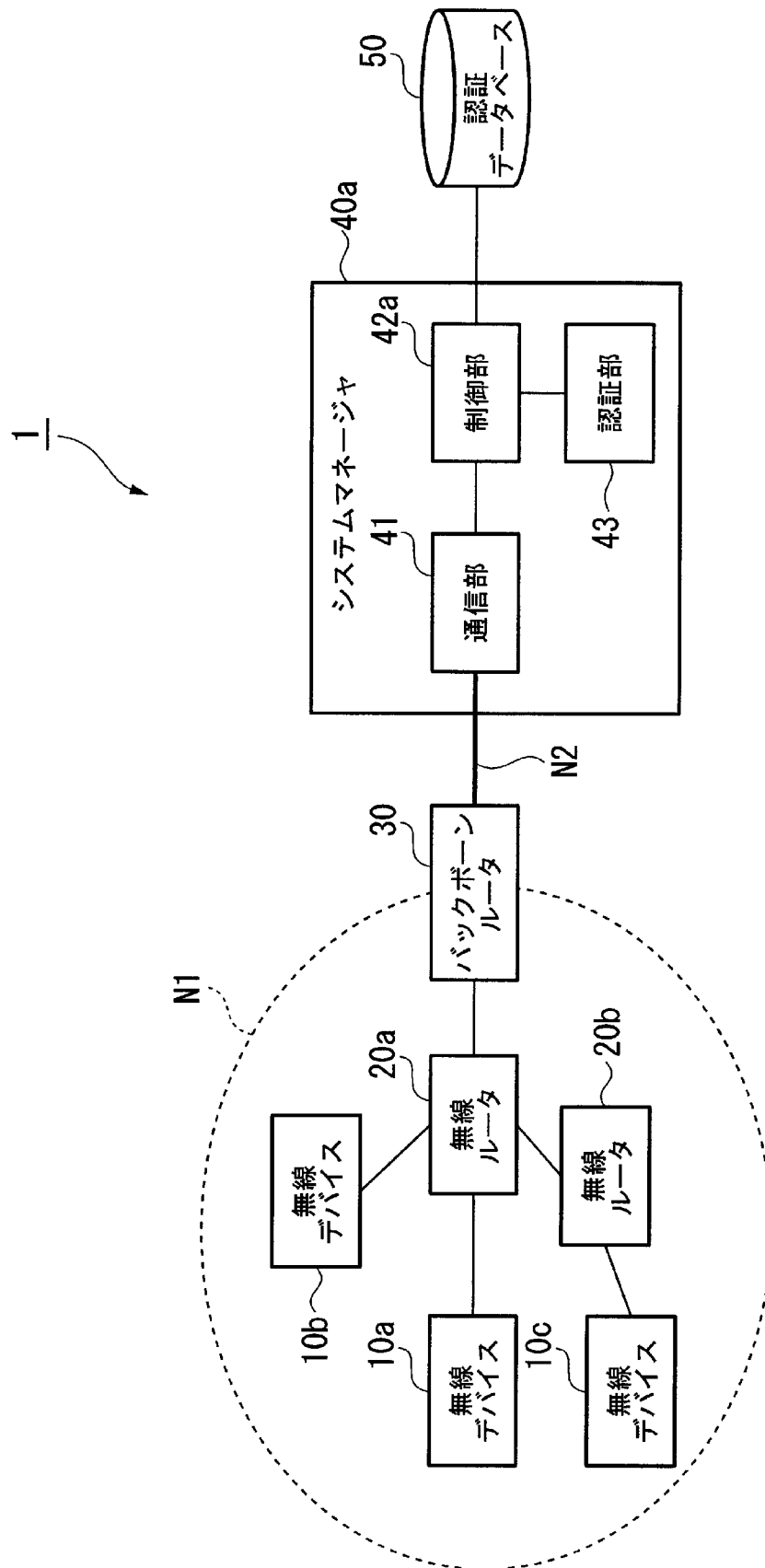
[請求項20]

ネットワークに接続される通信デバイスからの接続要求を受信し、

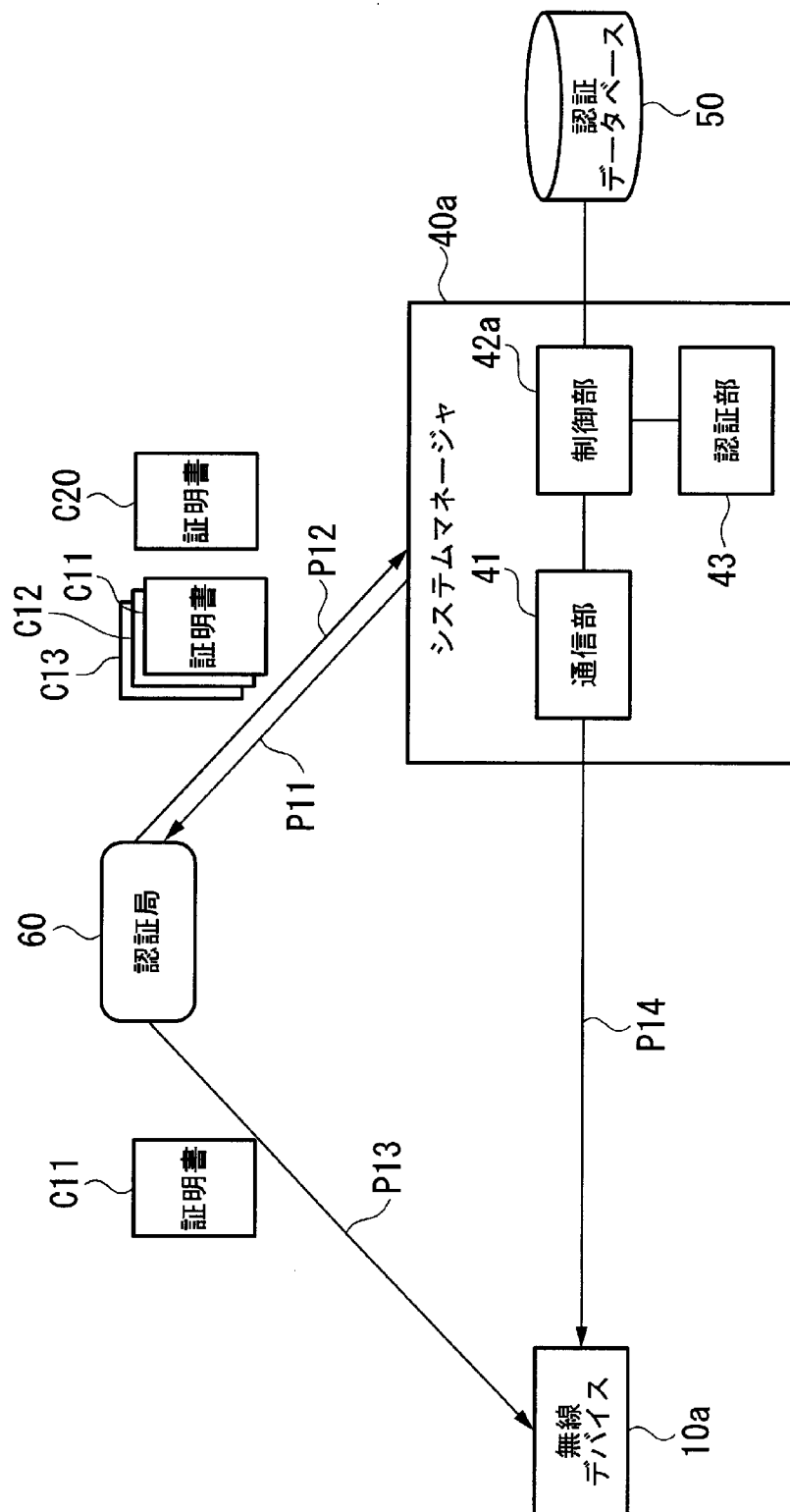
前記接続要求を受信した場合に、前記通信デバイスを認証するために用いられる第 1 証明書を格納するデータベースから、前記接続要求を行った前記通信デバイスを認証するための第 1 証明書を読み出し、

読み出した前記第 1 証明書を用いて、前記接続要求を行った前記通信デバイスの認証を行う認証方法。

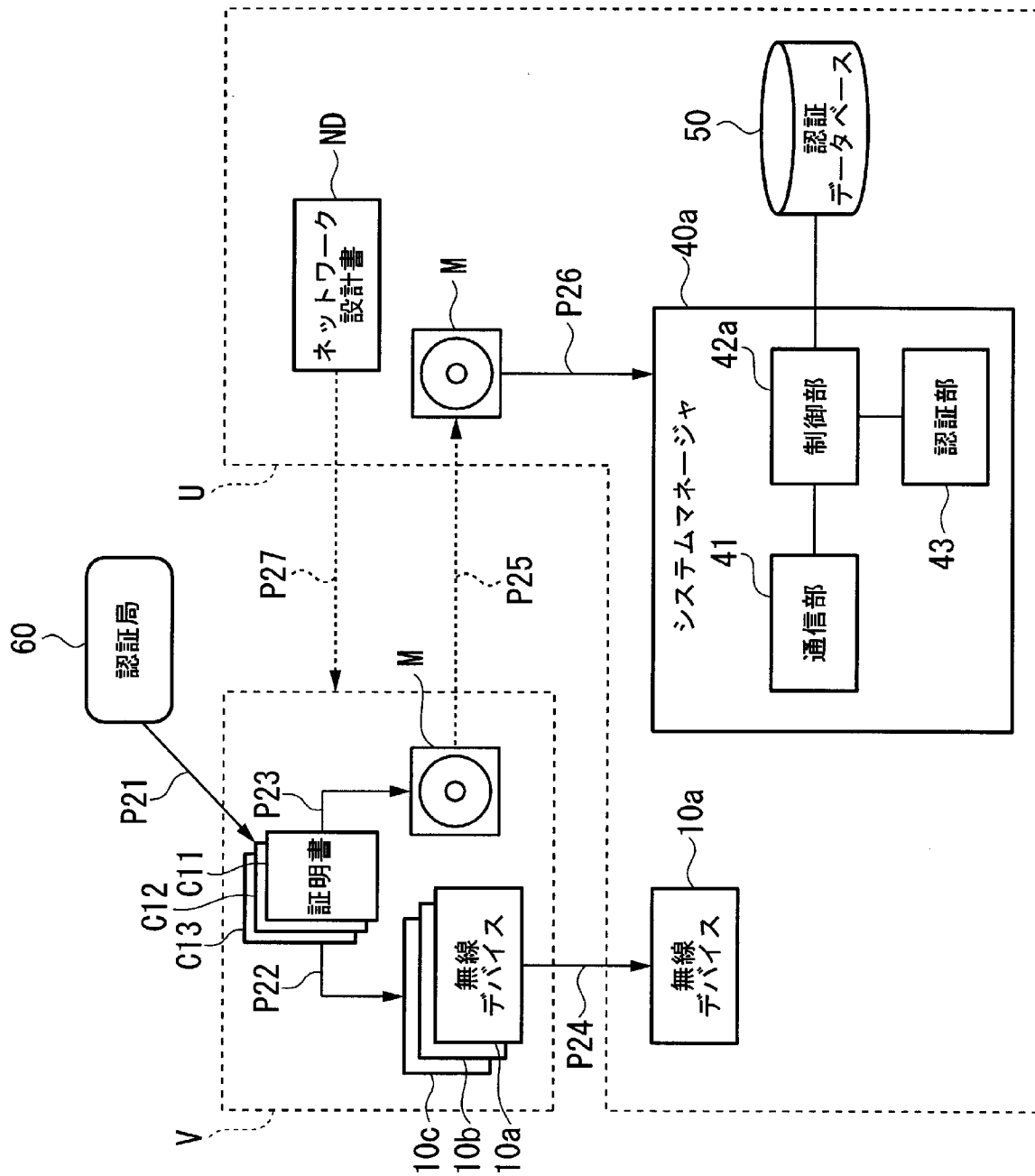
[図1]



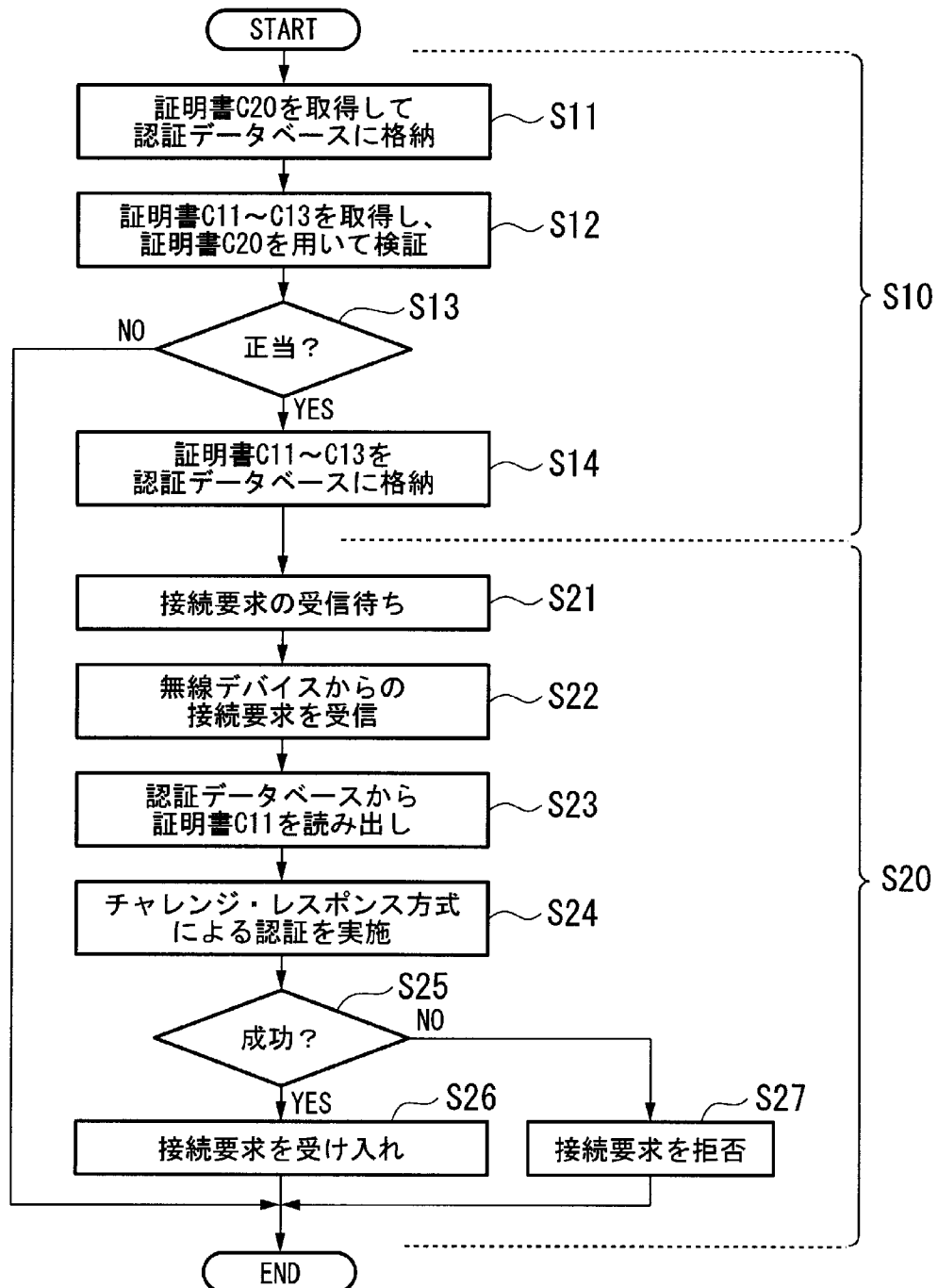
[図2]



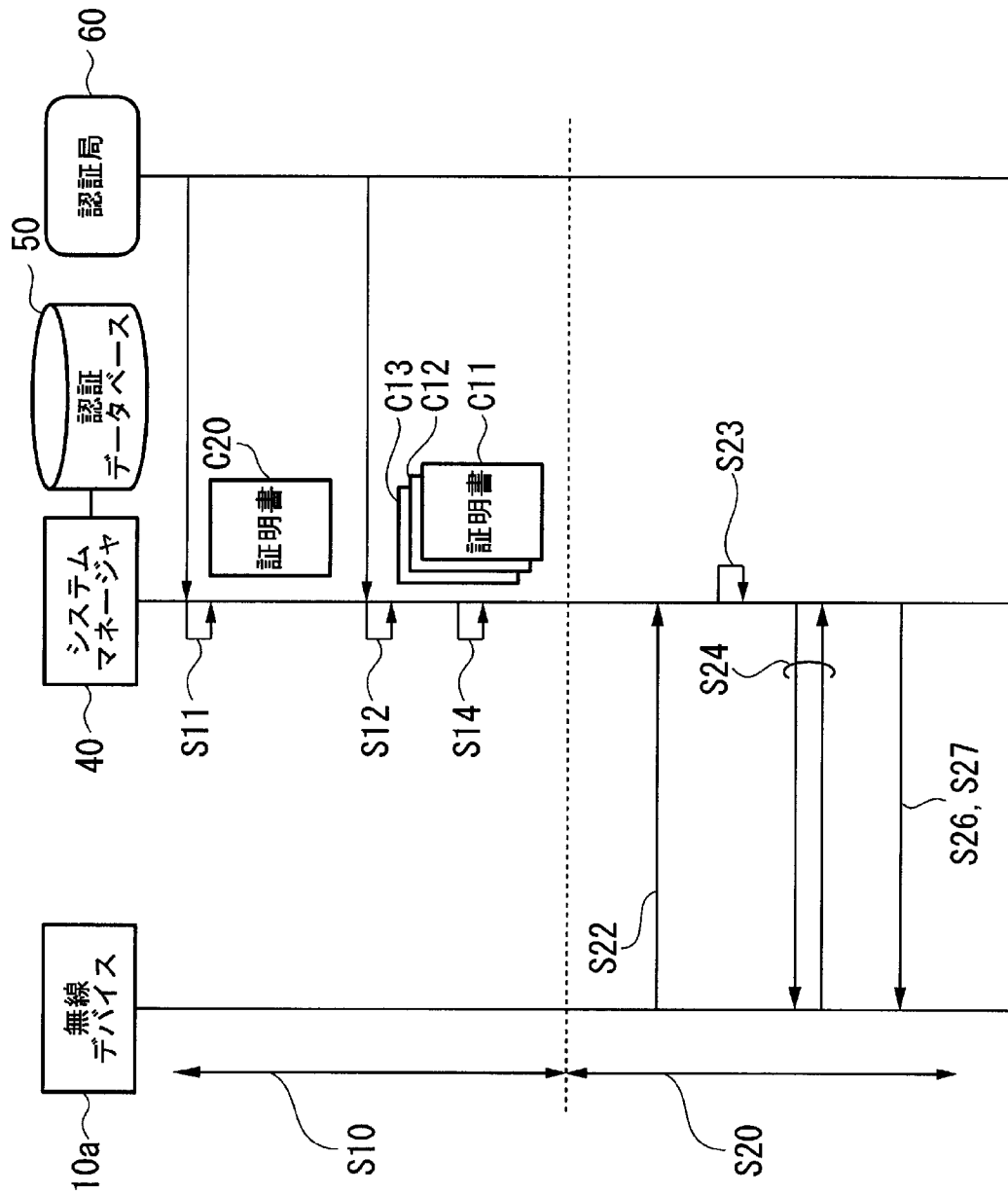
[図3]



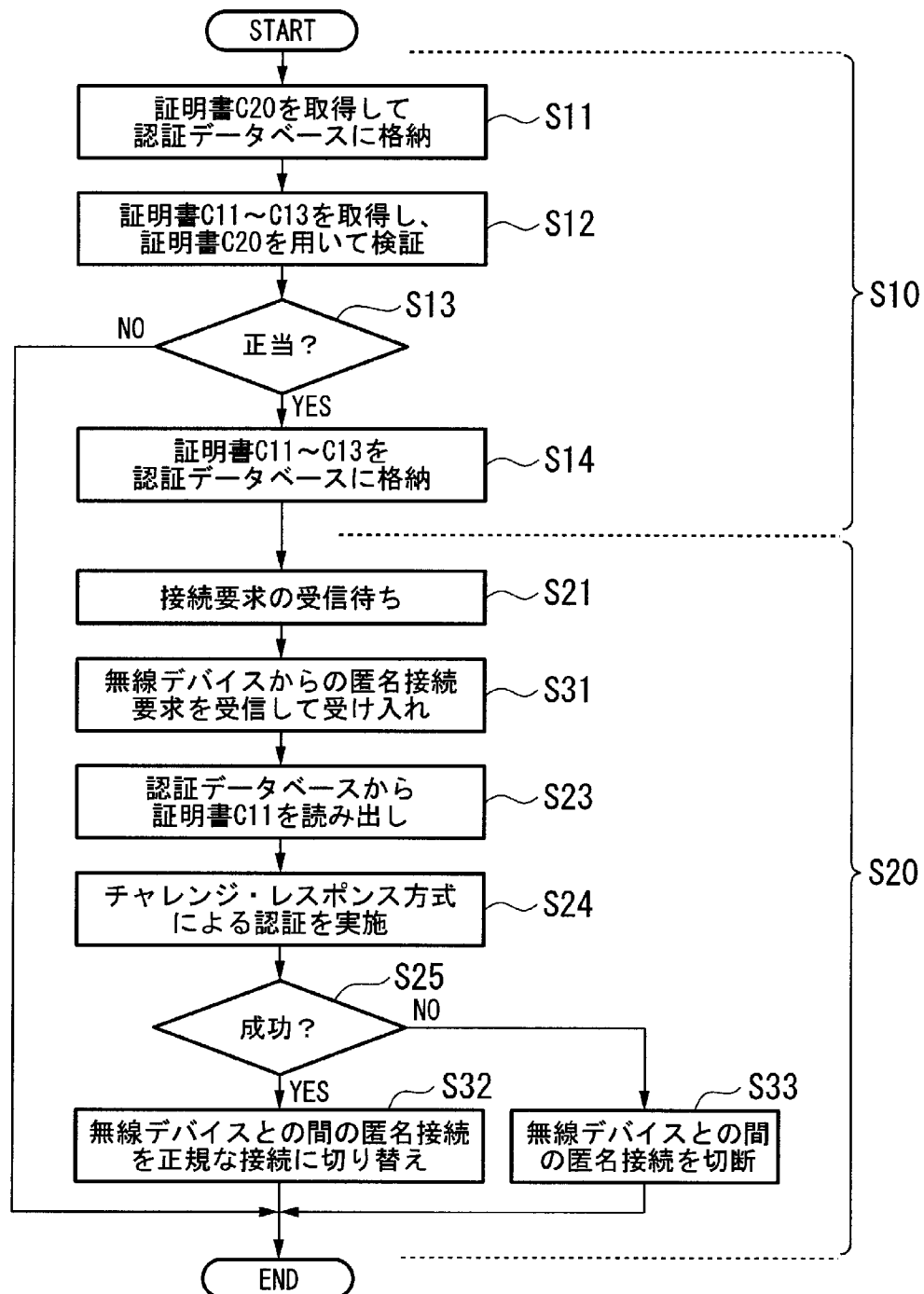
[図4]



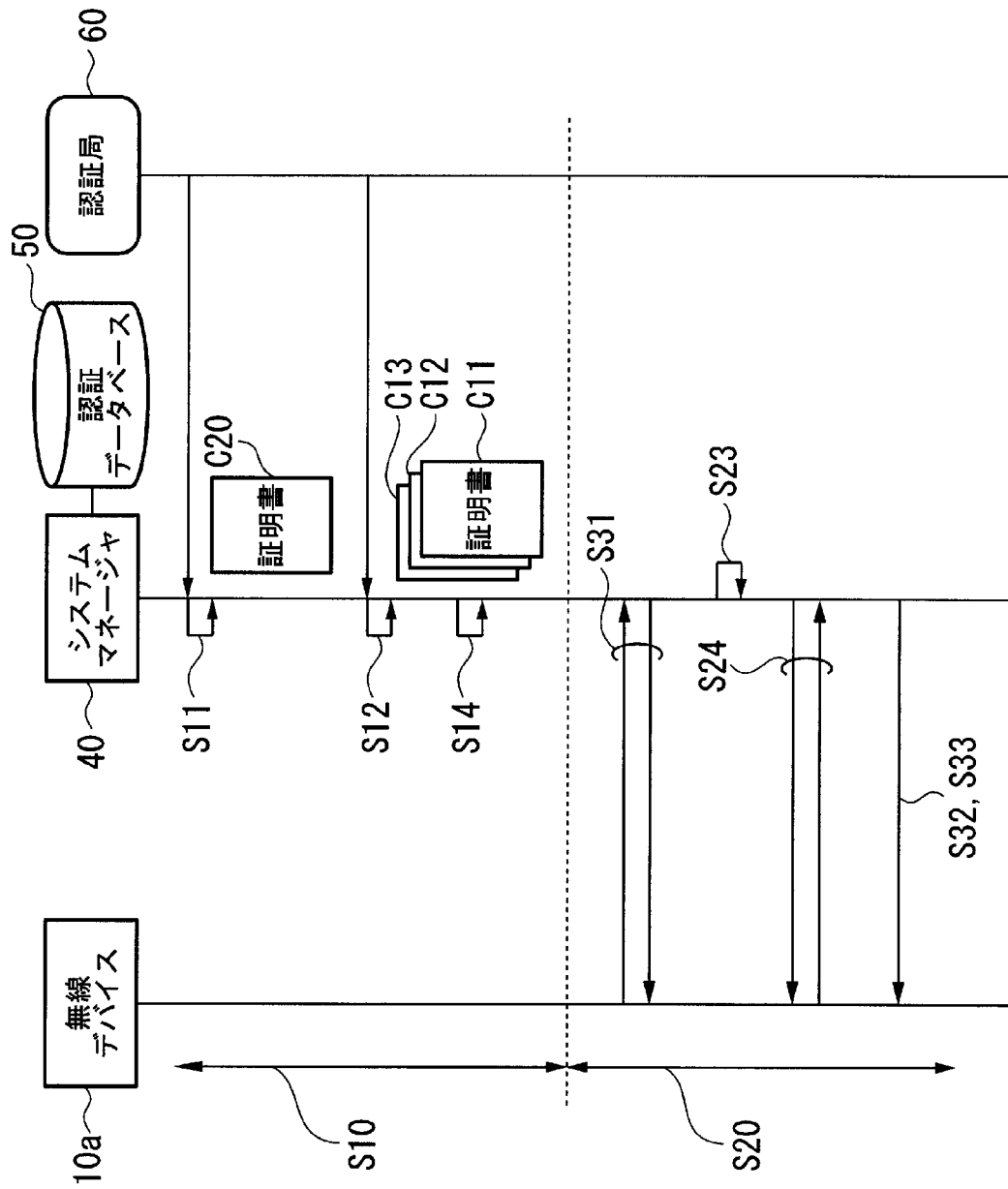
[図5]



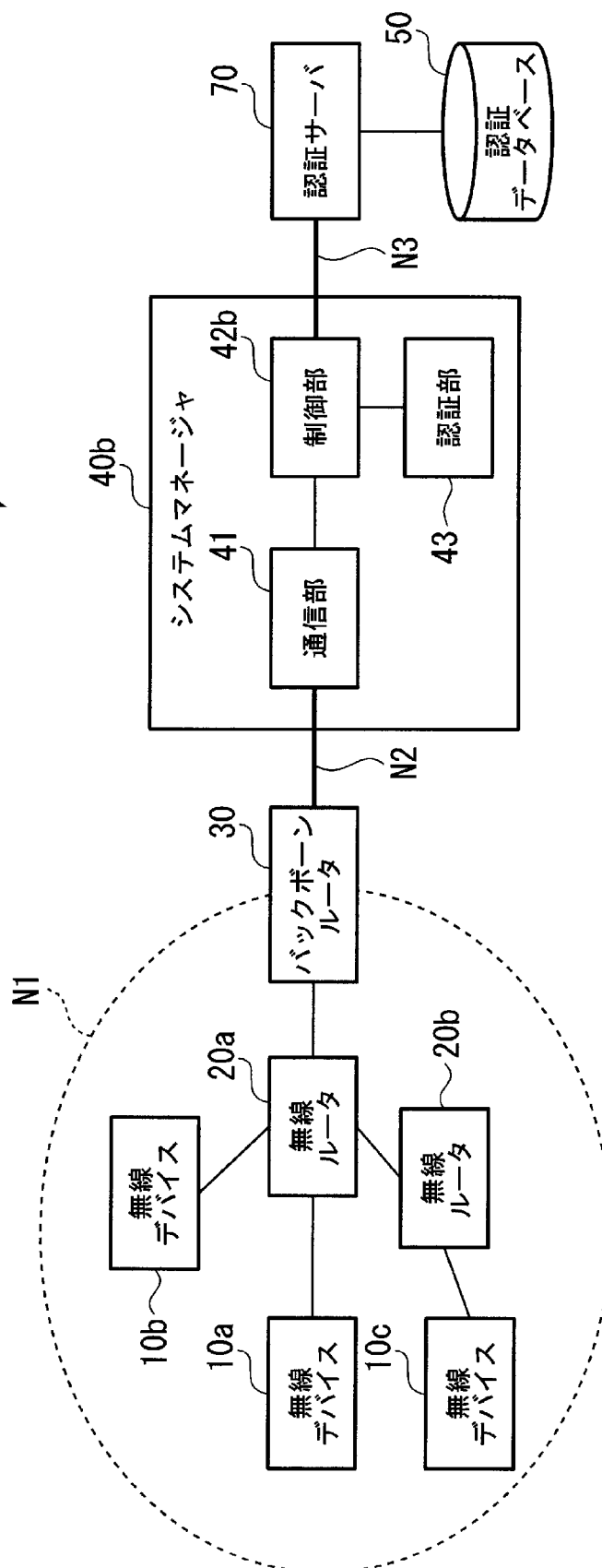
[図6]



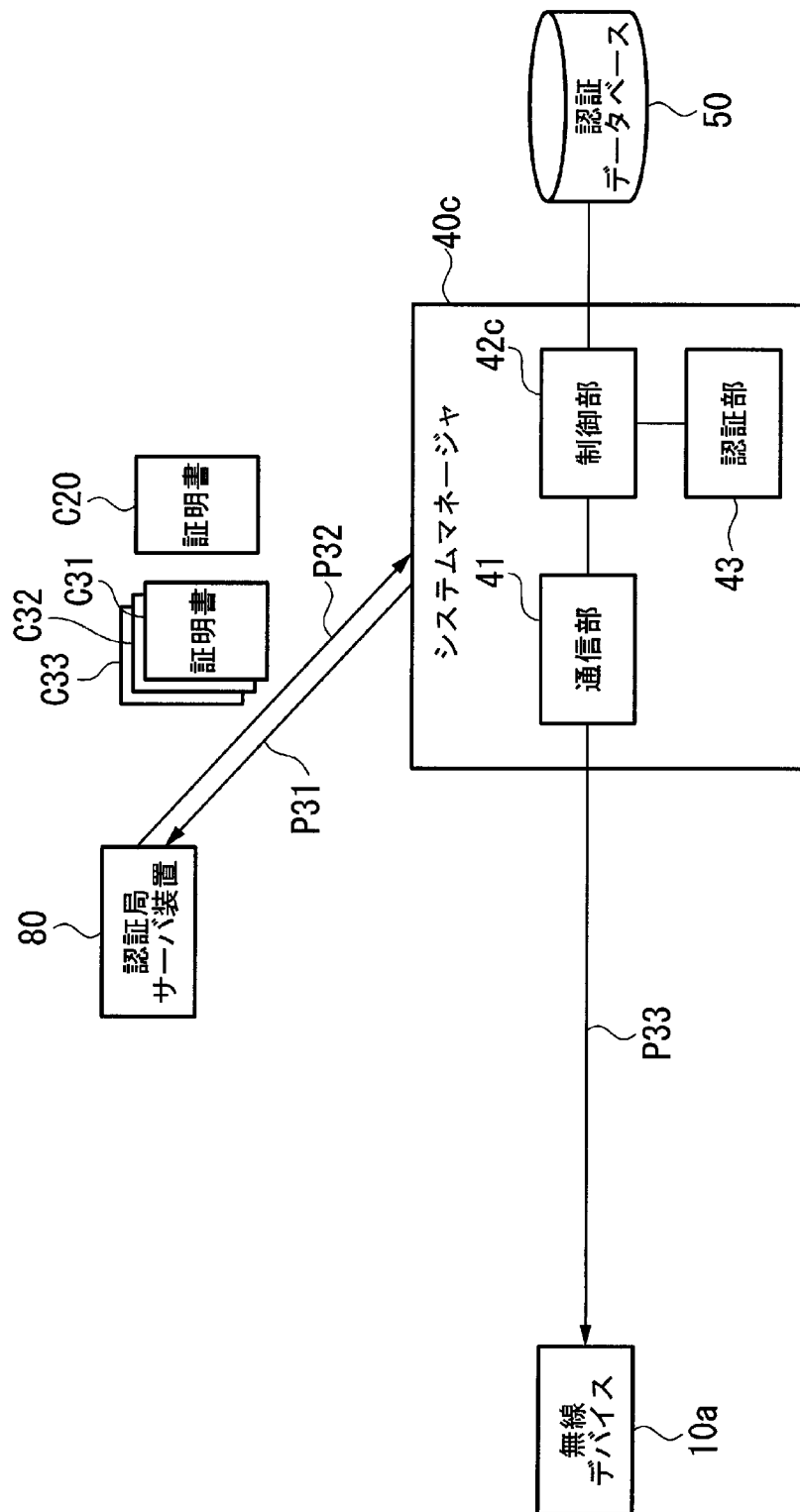
[図7]



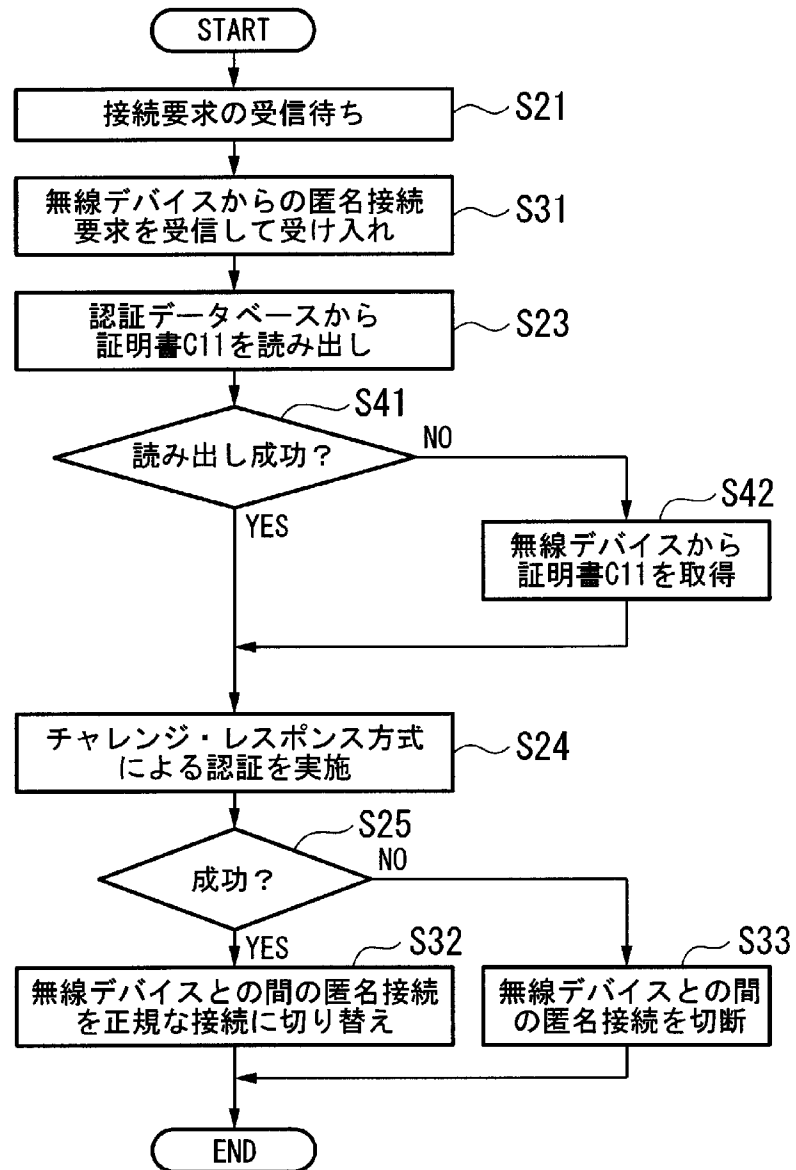
2/



[図9]



[図10]



INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP2013/072285

A. CLASSIFICATION OF SUBJECT MATTER

H04L9/32(2006.01)i, H04W12/06(2009.01)i

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

H04L9/32, H04W12/06

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Jitsuyo Shinan Koho	1922-1996	Jitsuyo Shinan Toroku Koho	1996-2013
Kokai Jitsuyo Shinan Koho	1971-2013	Toroku Jitsuyo Shinan Koho	1994-2013

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

JSTPlus/JMEDPlus/JST7580(JDreamIII), certificate, directory

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	JP 2002-501708 A (3Com Corp.), 15 January 2002 (15.01.2002),	1-4, 7, 8, 10, 12-15, 18-20
Y	page 8, line 5 to page 9, line 22; page 13, line 16 to page 15, line 15; page 16, line 11 to page 17, line 6; page 19, line 1 to page 20, line 15	5, 6, 9, 11, 16, 17
Y	JP 7-193569 A (Sun Microsystems, Inc.), 28 July 1995 (28.07.1995), paragraphs [0001], [0025] to [0047]	5, 6
Y	Blake-Wilson, S. et al., Transport Layer Security (TLS) Extensions, IETF RFC 4366, [online], 2006.04, [retrieval date 2013.10.24], The Internet <URL: http://www.ietf.org/rfc/ rfc4366.txt> especially 3.3. Client Certificate URLs	9

☒ Further documents are listed in the continuation of Box C.

☒ See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search
24 October, 2013 (24.10.13)

Date of mailing of the international search report
05 November, 2013 (05.11.13)

Name and mailing address of the ISA/
Japanese Patent Office

Authorized officer

Facsimile No.

Telephone No.

INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP2013/072285

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	JP 2006-59223 A (The Bank of Tokyo-Mitsubishi Ltd.), 02 March 2006 (02.03.2006), paragraphs [0018] to [0025], [0073] to [0079]	11
Y	JP 2000-508153 A (International Business Machines Corp.), 27 June 2000 (27.06.2000), page 9, line 4 to page 12, line 19	16,17
A	JP 9-219701 A (NCR International Inc.), 19 August 1997 (19.08.1997), paragraphs [0013] to [0017], [0023] to [0038]	1-20

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.

PCT/JP2013/072285

JP 2002-501708 A	2002.01.15	US 6311218 B1	2001.10.30
		EP 985298 A2	2000.03.15
		WO 1998/054869 A2	1998.12.03
		CA 2291760 A	1998.12.03
JP 7-193569 A	1995.07.28	US 5371794 A	1994.12.06
		EP 651533 A2	1995.05.03
JP 2006-59223 A	2006.03.02	(Family: none)	
JP 2000-508153 A	2000.06.27	US 5908469 A	1999.06.01
		EP 1055164 A2	2000.11.29
		WO 1998/038759 A2	1998.09.03
		TW 498278 B	2002.08.11
JP 9-219701 A	1997.08.19	US 5774552 A	1998.06.30
		EP 782296 A2	1997.07.02

A. 発明の属する分野の分類（国際特許分類（I P C））

Int.Cl. H04L9/32(2006.01)i, H04W12/06(2009.01)i

B. 調査を行った分野

調査を行った最小限資料（国際特許分類（I P C））

Int.Cl. H04L9/32, H04W12/06

最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報	1 9 2 2 - 1 9 9 6 年
日本国公開実用新案公報	1 9 7 1 - 2 0 1 3 年
日本国実用新案登録公報	1 9 9 6 - 2 0 1 3 年
日本国登録実用新案公報	1 9 9 4 - 2 0 1 3 年

国際調査で使用した電子データベース（データベースの名称、調査に使用した用語）

JSTPlus/JMEDPlus/JST7580(JDreamIII) certificate, directory

C. 関連すると認められる文献

引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求項の番号
X	JP 2002-501708 A（3コム コーポレーション）2002.01.15, 8頁5行-9頁22行, 13頁16行-15頁15行, 16頁11行-17頁6行, 19頁1行-20頁15行	1-4, 7, 8, 10, 12-15, 18-20
Y		5, 6, 9, 11, 16, 17
Y	JP 7-193569 A（サン・マイクロシステムズ・インコーポレイテッド） 1995.07.28, 1, 25-47 段落	5, 6

☒ C欄の続きにも文献が列挙されている。☒ パテントファミリーに関する別紙を参照。

* 引用文献のカテゴリー

「A」特に関連のある文献ではなく、一般的技術水準を示すもの
「E」国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの
「L」優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献（理由を付す）
「O」口頭による開示、使用、展示等に言及する文献
「P」国際出願日前で、かつ優先権の主張の基礎となる出願

の日の後に公表された文献

「T」国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの
「X」特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの
「Y」特に関連のある文献であって、当該文献と他の1以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの
「&」同一パテントファミリー文献

国際調査を完了した日

2 4 . 1 0 . 2 0 1 3

国際調査報告の発送日

0 5 . 1 1 . 2 0 1 3

国際調査機関の名称及びあて先

日本国特許庁（I S A / J P）
郵便番号 1 0 0 - 8 9 1 5
東京都千代田区霞が関三丁目4番3号

特許庁審査官（権限のある職員）

中里 裕正

5 S

9 3 6 4

電話番号 0 3 - 3 5 8 1 - 1 1 0 1 内線 3 5 4 6

C (続き) . 関連すると認められる文献		
引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求項の番号
Y	Blake-Wilson, S. et al., Transport Layer Security (TLS) Extensions, IETF RFC 4366, [online], 2006.04, [検索日 2013.10.24], The Internet <URL: http://www.ietf.org/rfc/rfc4366.txt > especially 3.3. Client Certificate URLs	9
Y	JP 2006-59223 A (株式会社東京三菱銀行) 2006.03.02, 18-25, 73-79 段落	11
Y	JP 2000-508153 A (インターナショナル・ビジネス・マシーンズ・コーポレーション) 2000.06.27, 9 頁 4 行-12 頁 19 行	16, 17
A	JP 9-219701 A (エヌシーアール インターナショナル インコーポレイテッド) 1997.08.19, 13-17, 23-38 段落	1-20

JP 2002-501708 A	2002.01.15	US 6311218 B1	2001.10.30
		EP 985298 A2	2000.03.15
		WO 1998/054869 A2	1998.12.03
		CA 2291760 A	1998.12.03
JP 7-193569 A	1995.07.28	US 5371794 A	1994.12.06
		EP 651533 A2	1995.05.03
JP 2006-59223 A	2006.03.02	ファミリーなし	
JP 2000-508153 A	2000.06.27	US 5908469 A	1999.06.01
		EP 1055164 A2	2000.11.29
		WO 1998/038759 A2	1998.09.03
		TW 498278 B	2002.08.11
JP 9-219701 A	1997.08.19	US 5774552 A	1998.06.30
		EP 782296 A2	1997.07.02